

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭62-166489

⑬ Int.Cl.⁴

識別記号

庁内整理番号

⑭ 公開 昭和62年(1987)7月22日

G 06 K 17/00
G 06 F 15/30
G 09 C 1/00

350

T-6711-5B
A-8219-5B
7368-5B

審査請求 未請求 発明の数 1 (全4頁)

⑮ 発明の名称 ICカードシステム

⑯ 特 願 昭61-7882

⑰ 出 願 昭61(1986)1月20日

⑱ 発 明 者 家 木 俊 温 横須賀市武1丁目2356番地 日本電信電話株式会社複合通信研究所内

⑲ 出 願 人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号

⑳ 代 理 人 弁理士 小林 将高

明 細 書

1. 発明の名称

ICカードシステム

2. 特許請求の範囲

ICカードおよびICカードの正当性のチェックを行うセンタより構成されるシステムにおいて、個々のICカード毎の特有値情報の正当性を保証するためのパスワードと、通信情報の暗号化・復号化を行うための暗号・復号関数および暗号・復号鍵を更新するための鍵更新関数と、これら暗号・復号鍵、鍵更新関数の固定・可変パラメータとを、個々の前記ICカードおよびセンタ内にそれぞれ格納し、かつ暗号・復号鍵の更新時に可変パラメータの変化値を前記ICカードに通知する通知手段を前記センタ内に設けたことを特徴とするICカードシステム。

3. 発明の詳細な説明

(産業上の利用分野)

この発明は、ICカードが、そのシステムのセンタに対して、パスワード等の情報を暗号化して

送信するICカードシステムに関するものである。

(従来の技術)

従来、ICカード内のパスワード(以下PWという)等の情報の暗号化に関しては、ICカードリーダがカードから読み取った情報を、専用の暗号装置で暗号化してからセンタに送る方法が提案されていた。しかし、この方法の場合、犯罪者が他人のカードを不正入手してカードリーダで読むと、カード内のIDコード(個々のICカード毎の特有値情報、以下IDという)、PWを知ることができる。その結果、そのID、PWを格納したカードの偽造、あるいはID、PWを端末のキーボードから入力しセンタに送信することによって、他人になりすまして不正取引をすることができた。

そこで、最近ではこのような問題を解決するため、カードが暗号関数を、センタが復号関数を格納し、さらに、暗号鍵の固定化を防止するため、センタからカードに対して暗号鍵を送信し、その

後、カードが暗号化を行う方式が提案されている。

第2図はこの方式の概要を示したものである。すなわち、第2図において、10はICカード、20はセンタを示し、ICカード10内には暗号器11を有し、センタ20内には復号器21と判別器22を備えている。ICカード10が端末に装着されると、センタ20から暗号鍵K、PW、IDを暗号器11に入力して暗号化PWつまりE(PW, ID, K)をセンタ20に送り、センタ20では復号器21で復号してPWをとり出し、センタ20内にあらかじめ記憶されているPWと照合を行い一致すれば取引許可の指令SAをICカード10側に送り、取引を開始させる。(発明が解決しようとする問題点)

しかし、この場合、ID、K、暗号化PWを通信回線より盗聴されると未知数がPWのみであるため、暗号関数を統計的処理等により見破られる可能性がある。

3

号化PWをセンタに送り、センタはこれから復号関数を生成し、センタ内で照合し、一致すれば取引許可信号をICカードに送る。

(実施例)

第1図はこの発明の一実施例の構成を示したブロック図である。この図で第2図と同じ符号は同じものを示し、12は前記ICカード10に設けた暗号鍵更新暗号器、23は前記センタ20に設けた復号鍵更新暗号器、24は通知手段で、センタ20からICカード10へ可変パラメータの変化値を通知する。

ICカード10内には、ID、PW、暗号関数E(X)に加えて、暗号鍵更新関数G(X)、G(X)の固定パラメータA、G(X)の可変パラメータR、i回目の取引に用いた暗号鍵K_iが格納されている。一方、センタ20には、ICカード10のID、PW、復号関数D(X)に加えて復号鍵更新関数H(X)、H(X)の固定可変パラメータB、R、i回目の復号鍵K_iが格納されている。なお、固定パラメータA、Bはあらかじめ

この発明の目的は、暗号鍵更新関数および個々のICカードに特有な更新関数の固定・可変パラメータをカード内に格納することにより、暗号鍵が犯罪者に見破られるのを防ぎ、システムのセキュリティを守ることにある。

(問題点を解決するための手段)

この発明にかかるICカードシステムは、個々のICカード毎の特有な暗号情報の正当性を保証するためのパスワードと、通信情報の暗号化・復号化を行うための暗号・復号関数および暗号・復号鍵を更新するための鍵更新関数と、これら暗号・復号鍵、鍵更新関数の固定・可変パラメータとを個々のICカードおよびセンタ内に格納し、かつ暗号・復号鍵の更新時に可変パラメータの変化値をICカードに通知する通知手段をセンタ内に設けたものである。

(作用)

この発明は、取引の度に暗号復号鍵を更新するための可変パラメータの変化値をセンタからICカードに送り、これに基づいてICカードから暗

4

め設定しておくもので、同じ値である必要はない。

次に動作について説明する。ICカード10からセンタ20にIDを送信すると、センタ20はICカード10に可変パラメータRの変化分ΔRを通知手段24から送信する。ICカード10は、暗号鍵更新関数G(X)に、K_i、R、ΔR、Aを代入して新たな暗号鍵K_i+1を生成し、これに基づいた暗号化PWをセンタ20に送信する。センタ20は、復号鍵更新関数H(X)に、K_i、R、ΔR、Bを代入して新たな復号鍵K_i+1を生成する。

その後、ICカード10は、暗号関数E(X)に、PWとK_i+1を代入して暗号化PWを生成し、センタ20を送信する。センタ20では、受信した暗号化PWを復号関数D(X)を用いて復号化しPWをとり出し、センタ20内のPWと照合し一致すれば取引許可信号SAを発し、金融取引等を許可する。なお、K_i、K_i'は一致させる必要はない。

5

6

この方式では、 ID 、 ΔR 、暗号化 PW を犯罪者が盗聴しても、 $E(X)$ 、 $G(X)$ 、 K_1 、 A 、 R が未知であるため、犯罪者が PW 、 $K_1 + 1$ を推測するのは不可能である。したがって、犯罪者が正しい暗号化 PW を生成し、他人になりすまして不正取引を行うことも不可能である。

なお、第1図の場合において、暗号関数 $E(X)$ と復号関数 $D(X)$ を同じにすれば（例えば、 PW と $K_1 + 1$ の排他的論理和をとる）、 $A = B$ 、 $K_1 = K_1'$ 、 $G(X) = H(X)$ となり、暗号方式の簡易化がはかれる。

（発明の効果）

この発明においては、同一システム内で利用される全ての IC カードは、全 IC カードに共通な暗号鍵更新関数と、各 IC カード固有の暗号鍵、関数用固定パラメータ、可変パラメータを IC カードとセンタ内に格納し、取引の度に暗号復号鍵を更新するための可変パラメータの変化値を送るようにしたので、以下の利点がある。

(1) IC カード内には、秘密の関数1個と、秘

密のパラメータが3つあり、これらを使って情報の暗号化を行うため、暗号化情報を解説されることはない。

(2) 犯罪者が暗号鍵を知る可能性がほとんどないため、暗号関数として、 IC カード内の CPU で実現できる簡易なものを用いることができる。

(3) 暗号関数として簡易なものを利用できるため、暗号化に要する時間が短くて良い。

(4) IC カードに固有な暗号鍵、パラメータを用いるため、1つの IC カードについて、犯罪者が秘密情報を知り得ても、他の IC カードについて知ることは不可能である。

4. 図面の簡単な説明

第1図はこの発明による IC カード利用システムの一実施例の構成を示すブロック図、第2図は、 IC カード利用システム用として従来提案されていた暗号・復号方式のシステムの構成を示すブロック図である。

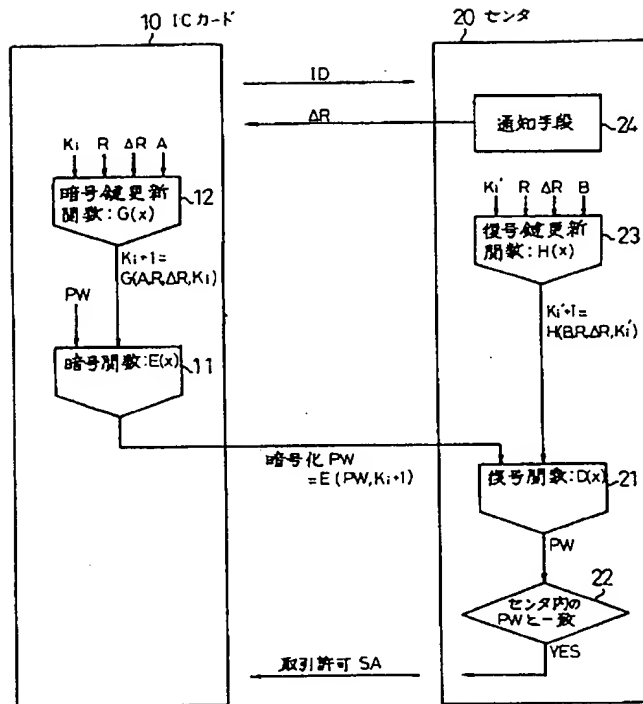
図中、10は IC カード、11は暗号器、12は暗号鍵更新暗号器、20はセンタ、21は復号

器、22は判別器、23は復号鍵更新暗号器、24は通知手段である。

代理人 小林 将 高



第 1 図



第 2 図

